(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11237969 A**

(43) Date of publication of application: **31.08.99**

(51) Int. Cl **G06F 3/12**
G06F 13/00

(21) Application number: **10329925**

(22) Date of filing: **19.11.98**

(30) Priority: **26.11.97 US 97 978793**

(71) Applicant: **INTERNATL BUSINESS MACH CORP <IBM>**

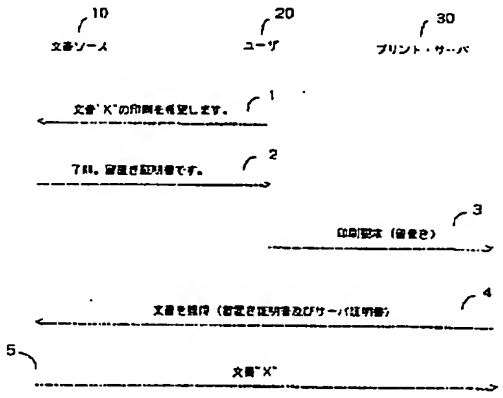
(72) Inventor: **ROGER K DEVRAY**

(54) **FILE PRINTING METHOD, NETWORK SYSTEM, COMPUTER SYSTEM, FILE SERVER AND PRINT SERVER**

(57) Abstract:

PROBLEM TO BE SOLVED: To enable a printer to directly retrieve a file from a file source based on authorization to a client by making a print server issue a certificate that guarantees authority for a print server to access a document.

SOLUTION: A user 20 requests a document source 10 for desire to print a document through communication 1. The source 10 or the owner of the document produces a keeping certificate based on the specific user's request and gives the keeping certificate to the requesting user through communication 2. The user 20 receives the keeping certificate, produces a print request and sends the print request to a print server 30 through communication 3. The server 30 requests the source 10 for the document through communication 4 and gives the keeping certificate verifying that a printer is allowed to acquire the document. After the source 10 confirms the printer and confirms that the certificate is not changed, it sends the document to the printer through communication 5.



(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3218017号
(P3218017)

(45)発行日　平成13年10月15日(2001.10.15)　(24)登録日　平成13年８月３日(2001.8.3)

(51)Int.Cl.[7]	識別記号	FI	
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｗ
			Ｄ
13/00	３５７	13/00	３５７Ａ
15/00	３３０	15/00	３３０Ｂ

請求項の数24(全 15 頁)

(21)出願番号　特願平10－329925
(22)出願日　平成10年11月19日(1998.11.19)
(65)公開番号　特開平11－237969
(43)公開日　平成11年８月31日(1999.8.31)
審査請求日　平成11年７月27日(1999.7.27)
(31)優先権主張番号　０８／９７８７９３
(32)優先日　平成９年11月26日(1997.11.26)
(33)優先権主張国　米国（ＵＳ）

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　ロジャー・ケイ・デブライ
アメリカ合衆国80503、コロラド州ロングモント、レイクビュー・サークル　3214
(74)代理人　100086243
弁理士　坂口　博　（外１名）

審査官　内田　正和

最終頁に続く

(54)【発明の名称】　ファイル印刷方法、ネットワーク・システム、コンピュータ・システム、ファイル・サーバ及びプリント・サーバ

(57)【特許請求の範囲】
【請求項１】インターネットを介して、ファイル・サーバに存在するファイルを印刷する方法であって、
第１のコンピュータ・システムにより前記ファイル・サーバに、前記ファイルを印刷する権限を要求するステップと、
前記要求に応答して、前記ファイル・サーバから前記第１のコンピュータ・システムに、前記第１のコンピュータ・システムのインターネット・アドレスを含む、前記ファイルを要求するためにプリント・サーバにより必要とされ、該プリント・サーバに転送される情報を含む証明書を発行するステップと、
前記証明書を前記第１のコンピュータ・システムから前記プリント・サーバに送信するステップと、
前記プリント・サーバから前記ファイル・サーバに、前記ファイルを要求し、前記ファイルを受信する権限として前記証明書を含むメッセージを送信するステップと、
前記証明書の内容から、含まれる前記証明書が、前記第１のコンピュータ・システムに発行されたのと同一の証明書であることを確認後、前記ファイル・サーバから前記プリント・サーバに前記ファイルを送信するステップとを含む、方法。
【請求項２】インターネットを介して通信接続される第１のコンピュータ・システム、プリント・サーバ及びファイル・サーバを含むネットワーク・システムであって、
第１のコンピュータ・システムにより前記ファイル・サーバに、ファイルを印刷する権限を要求する手段と、
前記要求に応答して、前記ファイル・サーバにより前記第１のコンピュータ・システムに発行され、前記ファイ

ル・サーバのデジタル署名及び前記ファイル・サーバのインターネット・アドレスを含む、前記ファイルを要求するために前記プリント・サーバにより必要とされる情報を含む証明書と、

前記第１のコンピュータ・システムから前記プリント・サーバに前記証明書を送信する手段と、

前記プリント・サーバから前記ファイル・サーバに、前記ファイルを要求し、前記ファイルを受信する権限として前記証明書を含むメッセージを送信する手段と、

前記ファイル・サーバにより前記証明書の内容から、含まれる前記証明書が、前記第１のコンピュータ・システムに発行されたのと同一の証明書であることを確認する手段と、

前記ファイル・サーバから前記プリント・サーバに前記ファイルを送信する手段とを含む、ネットワーク・システム。

【請求項３】第１のコンピュータ・システム内で実行される方法であって、

ファイル・サーバに存在するファイルをネットワークを介してリモート・プリンタにより印刷する要求を、前記ネットワークを通じて、前記ファイル・サーバに送信するステップと、

前記ファイル・サーバから前記ネットワークを通じて、前記ファイル・サーバのデジタル署名を含む、前記ファイルを印刷するための権限を受信するステップと、

前記権限を前記ネットワークを通じて前記プリンタに渡し、該プリンタが続いて前記ファイルを前記ファイル・サーバから直接フェッチし、印刷することを可能にするステップとを含む、方法。

【請求項４】ファイル・サーバに存在するファイルをリモート・プリンタにより印刷する要求を、ネットワークを通じて前記ファイル・サーバに送信する手段と、

前記ファイル・サーバから前記ネットワークを通じて受信され、前記ファイル・サーバのデジタル署名を含む、前記ファイルを前記ネットワークを通じて前記リモート・プリンタにより印刷するための権限と、

前記権限を前記ネットワークを通じて前記プリンタに渡し、該プリンタが続いて前記ファイルを前記ファイル・サーバから直接フェッチし、印刷することを可能にする手段とを含む、第１のコンピュータ・システム。

【請求項５】前記権限が前記ファイルの位置に関する情報を含む、請求項４記載のシステム。

【請求項６】前記権限が前記ファイル・サーバの識別名及び前記ファイルのパスを含む、請求項４記載のシステム。

【請求項７】ファイル・サーバ内で実行される方法であって、

第１のコンピュータ・システムからの、前記ファイル・サーバに存在するファイルへのアクセス権限に対する要求に応答して、第１のコンピュータ・システムからネットワークを通じてプリント・サーバに渡される、前記ファイル・サーバのデジタル署名を内容に含む権限の証明書を与えるステップと、

印刷のために前記ファイルへの直接アクセスを要求する前記プリント・サーバから、前記ネットワークを通じて、前記権限の証明書を受信するステップと、

前記証明書の内容を通じて、前記証明書が前記第１のコンピュータ・システムに与えられたのと同一の無変更の証明書であることを確認するステップと、

前記ファイルを前記プリント・サーバに送信するステップとを含む、方法。

【請求項８】リモート・プリント・サーバによるファイル・サーバに存在するファイルへの、ネットワークを介するアクセス権限のための要求を、第１のコンピュータ・システムから受信する手段と、

前記要求に応答して作成され、前記ファイルをアクセスするために前記プリント・サーバにより必要とされる情報及びデータ構造の妥当性を保証するために前記ファイル・サーバにより必要とされる情報を含む、コンピュータ読出し可能媒体上のデータ構造と、

前記データ構造を前記第１のコンピュータ・システムに送信する手段と、

印刷のために前記ファイルへの直接アクセスを要求する前記プリント・サーバから、前記ネットワークを通じて、前記データ構造を受信する手段と、

前記データ構造の内容を通じて、証明書が前記第１のコンピュータ・システムに送信されたのと同一の無変更のデータ構造であることを確認する手段と、

前記ファイルを前記プリント・サーバに送信する手段とを含む、ファイル・サーバ。

【請求項９】前記データ構造が前記ファイル・サーバのデジタル署名を含む、請求項８記載のファイル・サーバ。

【請求項１０】前記データ構造が前記ファイル・サーバの識別名、前記ファイルのパス、前記ファイル・サーバのデジタル署名、有効日及び前記ファイル・サーバにより作成された前記データ構造の固有番号を含む、請求項８記載のファイル・サーバ。

【請求項１１】前記データ構造が、前記要求内で指定されるプリント・サーバのプリンタＩＤ及びネットワーク・アドレスを含む、請求項８記載のファイル・サーバ。

【請求項１２】プリント・サーバ内で実行される方法であって、

第１のコンピュータ・システムのために、前記第１のコンピュータ・システムからネットワークを介して、ファイル・サーバからネットワークを介してファイルを検索し、前記プリント・サーバにより印刷するための要求を受信するステップと、

前記要求と共に、前記ファイルを突き止め、前記ファイルを検索して印刷する前記ファイル・サーバからの権限

を保証するために、前記プリント・サーバにより必要とされる情報を含む証明書を受信するステップと、
前記証明書を前記ネットワークを介して前記ファイル・サーバに送信するステップと、
前記ファイルを前記ファイル・サーバから受信するステップとを含む、方法。
【請求項１３】第１のコンピュータ・システムのために、前記第１のコンピュータ・システムからネットワークを介して、ファイル・サーバからネットワークを介してファイルを検索し、プリント・サーバにより印刷するための要求を受信する手段と、
前記要求と共に受信され、前記ファイルを突き止め、前記ファイルを検索して印刷する前記ファイル・サーバからの権限を保証するために、前記プリント・サーバにより必要とされる情報を含む、コンピュータ使用可能媒体上に存在するデータ構造と、
前記データ構造を前記ネットワークを介して前記ファイル・サーバに送信する手段と、
前記ファイルを前記ファイル・サーバから受信して印刷する手段とを含む、プリント・サーバ。
【請求項１４】前記権限を保証するために必要とされる情報が、前記ファイル・サーバのデジタル署名である、請求項１３記載のプリント・サーバ。
【請求項１５】第１のコンピュータ・システム、第２のコンピュータ・システム及び第３のコンピュータ・システムのネットワークを介して実行される方法であって、
前記第２のコンピュータ・システムから前記第１のコンピュータ・システムに、ファイル検索のための権限を要求するステップと、
前記要求に応答して、前記第１のコンピュータ・システムから前記第２のコンピュータ・システムに、前記ファイルを要求するために前記第３のコンピュータ・システムにより必要とされる情報を含み、前記第３のコンピュータ・システムに渡され、前記第１のコンピュータ・システムにより認証される証明書を発行するステップと、
前記第２のコンピュータ・システムから前記第３のコンピュータ・システムに、前記証明書及び前記ファイルの検索要求を送信するステップと、
前記第３のコンピュータ・システムから前記第１のコンピュータ・システムに、前記ファイルを要求し、該ファイルを受信する権限として前記証明書を含むメッセージを送信するステップと、
前記第１のコンピュータ・システムにより、含まれる前記証明書が、前記第２のコンピュータ・システムに発行されたのと同一で無変更の証明書であることを確認するステップと、
前記証明書が確認された場合、前記ファイルを前記第３のコンピュータ・システムに送信するステップとを含む、方法。
【請求項１６】印刷のために互いに通信リンクされる第

１、第２及び第３のコンピュータ・システムを有するネットワーク・システムであって、前記第３のコンピュータ・システムがプリンタを有し、ファイル・ソースを有するサーバとして機能する前記第１のコンピュータ・システムにファイルが存在するものにおいて、
前記第２のコンピュータ・システムから前記第１のコンピュータ・システムに、ファイルを印刷するための権限を要求する手段と、
前記要求に応答して、前記第１のコンピュータ・システムから前記第２のコンピュータ・システムに、前記ファイルを要求するために前記第３のコンピュータ・システムにより必要とされる情報を含み、前記第３のコンピュータ・システムに渡され、前記第１のコンピュータ・システムにより認証される証明書を発行する手段と、
前記第２のコンピュータ・システムから前記第３のコンピュータ・システムに、前記証明書及び前記ファイルの印刷要求を送信する手段と、
前記第３のコンピュータ・システムから前記第１のコンピュータ・システムに、前記ファイルを要求し、該ファイルを受信する権限として前記証明書を含むメッセージを送信する手段と、
前記第１のコンピュータ・システムにより、含まれる前記証明書が、前記第２のコンピュータ・システムに発行されたのと同一で無変更の証明書であることを確認する手段と、
前記証明書が確認された場合、前記ファイルを前記第３のコンピュータ・システムに送信する手段とを含む、システム。
【請求項１７】前記証明書が前記ファイルが記憶される位置の識別名を含む、請求項１６記載のシステム。
【請求項１８】前記識別名が前記ファイルが記憶される位置のインターネット・アドレスを含む、請求項１７記載のシステム。
【請求項１９】前記証明書が前記ファイルへのパスを含む、請求項１６記載のシステム。
【請求項２０】前記証明書が前記第１のコンピュータ・システムのデジタル署名を含む、請求項１６記載のシステム。
【請求項２１】前記第３のコンピュータ・システムがプリント・サーバである、請求項１６記載のシステム。
【請求項２２】前記第３のコンピュータ・システムが印刷システムである、請求項１６記載のシステム。
【請求項２３】前記第３のコンピュータ・システムがファックス・マシンである、請求項１６記載のシステム。
【請求項２４】前記第１のコンピュータ・システムが、前記ファイルが存在するファイル・データベースを含む、請求項１６記載のシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネット環

境などを含むコンピュータ・システムのネットワークに関して、特に、ネットワーク環境内の別々のファイル資源から検索されるファイルを確実に印刷することに関する。

【０００２】

【関連技術】本願は係属中の米国特許出願第９７９５０５号（ＩＢＭドケット番号ＡＭ９－９７－０５３）"SECURE CONFIGURATION OF A DIGITAL CERTIFICATE FOR A PRINTER OR OTHER NETWORK DEVICE"（本願と同日出願）に関連する。

【０００３】

【従来の技術】ネットワーク環境は無数の構成を含み得、それらにはＴＣＰ／ＩＰ接続やトークン・リング接続などを用い、インターネット、広域ネットワーク及びローカル・エリア・ネットワークに通信接続されるコンピュータ・システムが含まれる。同様に、コンピュータ・システム自体は、最小の記憶容量及びＣＰＵ処理機能を有するネットワーク端末からパーソナル・コンピュータに及び、後者にはラップトップ・コンピュータ、ワークステーション、サーバ及びメインフレームが含まれる。コンピュータ間の関係は、互いに独立であったり、或いは分散関係を有したり、クライアント／サーバ関係を有するなど、様々である。ファイルの一部または全てが、ファイル・サーバやデータベース管理システムなどの専用のファイル記憶システムに記憶されるか、或いは各システムの記憶装置内に記憶される。同様に、プリンタが任意のシステムまたは全てのシステムに接続されるか、或いはコンピュータ・システムと通信リンクされるプリント・サーバが存在し得る。

【０００４】ネットワーク環境内で発生する、多くの異なるタイプのセキュリティ問題が存在する。一部のファイルは、ファイル内容が伝送の間に無許可のエンティティにより傍受されないように、送信端で暗号化され、受信端で解読されなければならない。セキュリティ機構は、既知の他のセキュリティ機構と共に、ファイルがいたずらされないことを保証したり、送信者または受信者の識別を保証することができる。これらのセキュリティ機構の一部については以下で更に述べられる。

【０００５】暗号法：従来の暗号法、または換言すると従来の対称暗号法は、情報内容のプライバシを維持するために使用される。従来の暗号法は、暗号化メッセージの送信者及び受信者が秘密キーを共有することを要求する。情報をスクランブル（暗号化）及びスクランブル解除（解読）するために、同一のキーが使用される。１９７７年に、国家標準局（National Bureau of Standards）がデータ暗号規格（ＤＥＳ）と呼ばれるブロック暗号アルゴリズムを承認した。キーと共にＤＥＳアルゴリズムを用いることにより、２進コード化データが保護される。許可されたユーザは、データを解読するために、そのデータを暗号化するために使用されたキーを有さねばならない。ＤＥＳアルゴリズムを知り得るが、キーを知らない暗号化情報内容の無許可の受信者は、その情報内容を解読することができない。

【０００６】この方法による主な問題は、送信者及び受信者の両方がキーを有し、それ以外の者はキーを有さないことを保証することである。すなわち、キーの共有は、ある当事者がそれを他の当事者に送信することを要求する。しかしながら、ほとんどの通信ネットワークは信頼できないので、キー自身が暗号化されなければならない。キーが明文で送信されると、伝送路上で何者かがキーを傍受し、両当事者間で送信されるメッセージを復号し得る。他の場合ではキーを登録済みメールを介して送信するが、これは通信プロセスをスローダウンし、時間が問題とならない場合、メッセージ登録済みメールを単に送信することを前提とする。

【０００７】前述のように、無許可の受信者から情報内容を保護するため、キーが無許可のユーザから安全に保護される必要がある。従って、情報内容のセキュリティは、キーのセキュリティに依存する。キーはそれ自体、許可されたユーザに安全に配布されなければならない。

【０００８】公開キー暗号化：公開キー暗号化は、最初に１９７６年にスタンフォード大学のWhitfield Diffie及びMartin Hellmanにより紹介された。これは伝送されるメッセージのプライバシを保証するために使用されるだけでなく、デジタル署名などの他のアプリケーションにも使用され得る。

【０００９】伝送メッセージのプライバシを保証するために、公開キー暗号化が従来の暗号法で使用されるキーの安全な配布のための前述の多くの問題を解決する。公開キー暗号法は、私用キーと公開キーの２つのキーにもとづき、これらは協働して機能する。ある者の公開キーは他人に公に使用可能にされ、彼らの私用キーが秘密に保たれる。１つのキーが暗号化のために使用され、他のキーが情報内容を解読するために使用される。各暗号化キーに対して、それに対応する別々で異なる解読キーが存在する。ある者の公開キーにより暗号化されたメッセージは、その者の私用キーによってのみ解読され得る。たとえ一方のキーが知れても、他のキーを計算することは容易ではない。

【００１０】公開キー・システムでは、秘密キーを伝送すること無く、私的に通信することが可能である。例えば、各ユーザの暗号キーが配布または公開されることにより、公にされる。ある受信者と私的に通信したい者は、その受信者の公開キーに従い、単にメッセージを暗号化する。秘密解読キーを保持する受信者だけが、伝送されたメッセージを解読することができる。

【００１１】従来の暗号法及び公開キー暗号法の組み合わせは、秘密キーを目的の受信者に安全に送信することを可能にする。送信者は受信者の公開キーを用い、メッセージを秘密キーにより暗号化する。受信者はその受信

者の私用キーを用い、メッセージを解読し、また他の伝送の秘密キーを獲得する。公開キー暗号化は秘密キー暗号化よりも低速なので、このアプローチは、続く伝送がより高速な従来の秘密キー暗号法アプローチを使用することを可能にする。

【００１２】デジタル署名：これらの暗号システムでは、時に、受信されたメッセージの送信者が、実際に、メッセージ内で命名された人物であるか否かを確認する必要がある。公開キー暗号法にもとづくデジタル署名が、メッセージの送信者を認証する手段として使用される。デジタル署名はデジタル・メッセージの署名を可能にし、それにより、デジタル的に署名された電子メッセージの任意の受信者は、メッセージの送信者を認証し、署名されたメッセージの完全性を確認することができる。すなわち、受信者はメッセージが送信通りに受信され、またメッセージが偽造でないことを保証される。

【００１３】元の真の送信者がメッセージを送信したことを保証するために、前述の公開キー暗号法を用いる私用通信を保証するために使用されるプロセスと、正反対のプロセスが使用される。例えば、公開キーを公にしたユーザは、メッセージを伝送する前に、そのメッセージまたはメッセージのハッシュをユーザの私用キーにより暗号化することにより、メッセージにデジタル的に署名できる。メッセージの受信者は、メッセージまたは署名を送信者の公開暗号キーにより解読することにより、それらを確認できる。このプロセスは、メッセージが最初に送信者によりその私用キーを用いて暗号化され、受信者により送信者の公開キーを用いて解読されるという点で、従来の暗号法と正反対である。送信者の公開暗号キーを有する者は、メッセージまたは署名を読むことができる。任意のこうした受信者は、メッセージの作成者の認証を保証される。なぜなら、秘密私用キーを有する送信者だけが、メッセージまたは署名を作成し得たからである。受信者はまた、メッセージが最初に作成されて以来、それが変更されておらず、デジタル署名がそれに付け加えられたことを保証される。任意の受信者が、署名者の公開キーだけを用いることにより、デジタル署名を認証でき、メッセージの完全性を確認できる。

【００１４】前述の例では、デジタル署名が、送信者の私用キーを用いることによるメッセージ自体の暗号である。デジタル署名規格（ＡＮＳＩ　Ｘ９．３０パートＩ）では、人のデジタル署名が固定長ビット・ストリングであり、任意の長さの電子メッセージに付け加えられる。固定長デジタル署名を作成するために、任意長のメッセージを、同一の固定長ハッシュまたはダイジェストのメッセージに変換するハッシュ関数が使用される。セキュア・ハッシュ・アルゴリズム（ＳＨＡ）は、デジタル署名規格の一部である既知のハッシュ関数である。メッセージのこのハッシュは、２つの別個のメッセージが同一のハッシュを生じることが実際に不可能である点で、"指紋"に似ている。メッセージのハッシュを作成後、送信者の私用キーがハッシュに付け加えられ、メッセージのデジタル署名が作成される。デジタル署名は、署名されるメッセージ及び署名者の私用キーの両方の関数である。私用キーが秘密に守られる限り、デジタル署名が他人により作成されることはない。

【００１５】デジタル的に署名されたメッセージの受信に際して、受信者は送信者の公開キーを用い、デジタル署名を送信者が計算したハッシュに変換する。次に、受信者は同一のハッシュ関数を受信された平文メッセージに適用し、受信メッセージのハッシュを獲得する。受信されたメッセージのハッシュが、デジタル署名を変換するために送信者の公開キーを用いて獲得されたハッシュと同一の場合、受信者は送信者のデジタル署名を認証し、署名されたメッセージの完全性を確認したことになる。

【００１６】証明書：署名者の識別は、公開キーが実際にそれらしい送信者に帰属することを、受信者が確信する程度に保証するに過ぎない。この問題を解決する１つの既知の技術は、例えば政府機関などの特定の信頼される当局に頼ることにより、各公開キーが所有者であると主張する当人に関連付けられるように保証することである。信頼される当局が、主張者の公開キー及び主張者の名前を含む証明書（certificate）として知られるデジタル・メッセージを作成する。当局の代表は、デジタル・メッセージに当局自身のデジタル署名を署名する。当局のデジタル署名は当局の私用キーを用いて作成され、受信者により当局の公開キーを用いて解読される。こうした公開キーは、電話帳、新聞及びインターネット・ウェブ・ページなどを通じて広く普及され、入手可能である。この証明書は、送信者のメッセージ及び送信者のデジタル署名と一緒に送信される。受信者は当局の公開キーを用いて証明書を解読し、送信者の認証された公認の公開キーを見い出す。受信者は次に送信者の公認の公開キーを用い、送信者の署名されたメッセージを確認する。従って、証明書は容易に認証され、メッセージの完全性が確認され得る。

【００１７】証明書を使用するアクセス制御：通常、別のシステムまたはユーザ（"user"）からコンピュータ・システム（"server"）の資源へのアクセスは、パスワードを通じて制御される。このことはサーバが全ての許可されたユーザ、並びに各ユーザのパスワードのデータベースを保持することを要求する。しかしながら、ユーザが別の無許可のユーザとパスワードを共有する場合、パスワード・アクセス制御システムの完全性が損なわれる。

【００１８】証明書ベースのアクセス制御システムでは、サーバは認可当局により発行された証明書を認証するだけでよい。サーバは、ユーザまたはユーザの対応するパスワードに関するデータベースを保持する必要がな

い。サーバの資源へのアクセスを獲得するために、ユーザはユーザの証明書を提示する。偽造され得ないデータを含む証明書から、サーバはユーザの認証された公開番号、個人データ及びアクセス特権を獲得できる。サーバは次に、ユーザにランダム・メッセージを伝送でき、ユーザはそれに自分の専用番号をデジタル的に署名し、サーバに返却しなければならない。サーバは次に、証明書内の公開番号を用いてデジタル署名を認証し、署名済みメッセージが自身がユーザに送信したものと同一であることをチェックできる。このデジタル的に署名された応答により、サーバはユーザが証明書内の認証済み公開番号に対応する正しい専用番号を有するか否かを決定できる。

【００１９】送信者と受信者間の保護された伝送：前述の安全な伝送技術は、送信者と目的のユーザ間でメッセージまたはファイルが直接伝送される状況において最適である。

【００２０】任意のネットワーク環境では、ユーザ（端末またはシステム上で実行されるアプリケーションを介して、システムと対話する個人）が、ユーザから遠隔的に配置される文書を印刷したい状況が発生し得る。文書は、アクセス特権を有するユーザ以外の者によるアクセスから保護され得る。

【００２１】通常、ユーザはリモート・システムから文書を要求し、リモート・システムはユーザが正しいアクセス特権を有するか否かを確認し、もしそうであれば、リモート・システムが文書のコピーをユーザに送信する。ユーザは次にファイルを印刷のためにプリンタに送信する。しかしながら、アクセス特権を有するこうしたユーザは、文書をリモート・プリンタまたはプリント・サーバ上で印刷することを希望し、最初に文書をユーザ自身のローカル・コンピュータ・システム（便宜上クライアント・システムと呼ばれる）において、検索及び記憶することを希望しないかも知れない。様々な理由から、ユーザは文書をユーザ自身のマシン上に有することを希望しないかも知れない。例えば、これらの理由には、次に挙げる任意の１つまたは幾つかが含まれ得る。すなわち、クライアント・システムが安全な環境にない、ネットワーク・トラフィックの問題点が存在する、或いはクライアント・システムがファイルなどを受信する記憶空間を有さないなどである。更に、ファイル・サーバは、ファイルのコピーがクライアント・システム上に記憶されることを望まないかも知れない。ファイル（例えば文書）の所有者は、例えば文書の著作権または１コピー当たりの料金の支払いを保護するために、分配されるコピの一数を管理したいかも知れない。コピーがクライアント・マシン上に存在する場合、違法なコピーが更にそのコピーから作成されたり、違法な変更が文書に行われたりし得る。代わりに、プリンタが文書をそれが記憶され得る場所から直接獲得し、その文書を印刷すれば、より望ましかろう。

【００２２】しかしながら、これを実行するためには、文書がアクセスを保護されている場合、プリンタはユーザが有するアクセス特権と同一のアクセス特権を有する必要がある。

【００２３】元来プリント・ファイルを要求したクライアント・システムにより、最初にファイルが獲得されることなく、文書が印刷されるように、プリント・サーバがプリント・ファイルをオリジナル要求内で識別される第３者から獲得する必要性が存在する。しかしながら、プリント・サーバがファイルを獲得するとき、第３者は要求が有効である（すなわち、プリント・サーバがファイルの獲得を許可されており、オリジナル・クライアントが正当に文書を印刷できる）ことを保証されなければならない。こうした状況が、既存のプロトコルの下で可能なことが知られていない。

【００２４】

【発明が解決しようとする課題】従って、本発明の目的は、クライアントからの要求に応じて、ファイル・ソースからクライアントへの権限付与にもとづき、プリンタがファイル・ソースから直接ファイルを検索することを可能にすることである。

【００２５】本発明の別の目的は、"参照による印刷（print by reference）"操作を要求しているユーザと同一のアクセス特権を、プリンタに提供することである。

【００２６】用語"参照による印刷"は、ここでは次の印刷状況、すなわちユーザが実際に文書を検索し、印刷のための文書のターゲット・コピーとして使用するために、その文書をユーザ自身のローカル・コンピュータに記憶することのない印刷状況を指し示すために使用される。

【００２７】

【課題を解決するための手段】本発明のシステム、方法及びプログラムは、ユーザすなわちクライアント・システムが、ファイル・ソースからファイルを検索及び印刷する権限をプリンタに受け渡すことを可能にする。この状況は、代理人の本人（principal）のために、イベントのチケットを要求する代理人に類似する。代理人が本人の名前をチケット販売所に申し出て、注文番号を受け取る。代理人は注文番号を本人に与える。本人は次にイベントの時刻にチケット販売所の"留置き（will-call）"窓口に出向き、チケットを受け取るために注文番号及び本人のＩＤをチケット販売所に提示する。チケット販売所は、信頼される当局すなわち政府により発行された自動車免許証などの本人のＩＤにより、その本人が誰であるかを知り、その本人がチケットを与えるべき対象者であることを認識する。なぜなら、代理人は最初の要求において本人を識別しており、本人がその初期要求に正しく対応した注文番号を提示したからである。

【００２８】ネットワーク印刷環境では、クライアント

が文書の印刷を要求するとき、文書ソース（ファイル・ソース）が"留置き"証明書をクライアントに発行する。"留置き"証明書は、文書をアクセスし、文書が第3者すなわちプリント・サーバに渡されることを許可する権限を保証する。留置き証明書はファイル・ソースにより作成され、その内容はファイル・ソースへの初期ユーザ要求にもとづく。証明書は、印刷データを要求するためにプリント・サーバにより必要とされる情報、例えば文書が記憶される場所の識別名及び文書を含むファイルへのパスなどを提供する。留置き証明書はまた、プリンタによりファイル・ソースに提示される任意のこうした留置き証明書が、正当なものであることをファイル・ソースが確認するための情報を含む。例えば、留置き証明書は、ファイル・ソースのデジタル署名を含む。デジタル署名は、留置き証明書の他の内容に対してハッシュ関数を用いることによる、その特定の要求に固有の署名（前述の類比における注文番号に類似）である。デジタル署名は、ファイル・ソースによってのみ知られる私用キーを用いて作成される。留置き証明書はまた、プリンタのプリンタＩＤ及びネットワーク・アドレスを含み得、ユーザはこれをファイル・ソースへの初期要求内で、ファイルを検索及び印刷するプリンタとして指定する。留置き証明書はまた、初期要求を生成するユーザＩＤを含み得る。

【００２９】クライアントは、このファイルを印刷する要求と一緒に、留置き証明書をプリンタに送信する。プリンタはデータを印刷する準備が整うと、メッセージを留置き証明書と一緒に、文書を要求する文書ソースに送信する。文書を獲得するためのプリンタの権限は、留置き証明書である。証明書はファイル・ソースのデジタル署名を含むので、留置き証明書の偽造は可能でない。また、プリンタが留置き証明書をファイル・ソースに提示するとき、ファイル・ソースは、留置き証明書内に含まれるファイル・ソースのデジタル署名に対して、プリンタがユーザにより最初に識別されたプリンタであり、プリンタが同一のネットワーク・アドレスであることを確認できる。プリンタはまた留置き証明書と一緒に、プリンタのデジタル証明書をファイル・ソースに送信し、それによりファイル・ソースは、そのプリンタがそれが主張する当該プリンタであることを確認できる。こうしたデジタル証明書は、前記米国特許出願第９７９５０５号（ＩＢＭドケット番号AM９－９７－０５３）に従い構成される。

【００３０】留置き証明書を組み込む他の実施例には、サーバに暗号文（cryptolope）にて送信される"購入"文書が含まれる。

【００３１】

【発明の実施の形態】本発明のシステム、方法及びプログラムは更に、ユーザ（クライアント）２０、文書ソース１０及びプリント・サーバ３０の間の情報の流れを示す図１に関連して後述される。図示のように及び後述されるように、"留置き"証明書がこれらの通信の一部内に含まれる。ユーザ（クライアント）は、ネットワーク・ステーション、ワークステーション、または任意のタイプのコンピュータ・システム上で実行されるアプリケーション・プログラムを通じて対話するユーザである。プリント・サーバは、ネットワークに接続されるか、またはプリンタの機能を管理するコンピュータであるサーバに直接接続されるスタンドアロン・プリンタと、こうした管理に専ら捧げられるコンピュータとして、またはこうした管理に加え、他のタスクを実行するコンピュータとしてキュー待機する装置とを含む。同様に、ファイル・ソースは、例えばシステムの記憶装置上のファイルの管理に専ら捧げられるコンピュータ・システムである。こうしたファイル・サーバは、データベース管理システムまたはデジタル・ライブラリなどを含み得る。

【００３２】本発明のシステム、方法及びプログラムは、文書ソース１０に移行し、通信１を介して文書を印刷する希望を要求する能力をユーザ２０に提供する。本発明は、ユーザが文書を印刷する権利を獲得するために、料金を支払わねばならなかったり、或いは文書へのアクセスを獲得するために、パスワードを提供しなければならない状況を考慮する。これらの状況は後述の他の実施例で述べられる。

【００３３】文書を印刷する要求を受信すると、文書ソース１０または文書の所有者が、その特定のユーザ要求にもとづき、留置き証明書を作成し、要求するユーザに通信２を介して留置き証明書を与える。

【００３４】留置き証明書４０（図２）は次のフィールド、すなわち、文書を獲得するために移行すべき場所（例えばインターネット・アドレスを含む）を、プリント・サーバに正確に伝える文書ソースの識別名４１、ファイル・システム内で文書を見い出すための文書ファイルへのパス４２及び文書のプロバイダのデジタル署名４３を含む。文書ソースが留置き証明書を作成するとき、文書ソースはそれ自身の私用キーを用い、留置き証明書にデジタル的に署名する。留置き証明書はまた、証明書が有効な日付４４及び追跡目的のための通し番号４５を含む。通し番号は、ファイル・ソースにより発行される各留置き証明書に対して固有である。この固有の通し番号もまた、"留置き"ベースでチケットを要求するときに与えられる注文番号と類似に、ファイル・ソースにより追跡目的のために使用され得る。

【００３５】留置き証明書は更に、ファイルの印刷を要求するユーザのユーザＩＤ及びプリンタＩＤ、更にファイルを検索及び印刷するためにユーザにより使用されるプリンタのネットワーク・アドレスを含むフィールドを含み得る。留置き証明書はまた、パスワードもしくは他の秘密情報、またはキーを含み得る。

【００３６】図１を参照すると、ユーザ２０は"留置き"

証明書を受け取り、印刷要求を生成し、通信３を介して印策要求をプリント・サーバに送信する。印刷要求は、どの文書が要求されているか及びその文書がどこにあるかを指定する。要求はまた、文書ソースに移行し、文書を獲得するための資格証明をプリンタに与える"留置き"証明書を含む。

【００３７】プリント・サーバ３０は文書ソース１０に移行し、通信４を介して文書を要求し、文書ソースにプリンタがその文書を獲得することを許可されていることを立証する留置き証明書を与える。プリント・サーバはまた文書ソースに、サーバ証明書またはデジタル証明書を与える。本発明の好適な実施例で使用されるこうした証明書の１つが、前記米国特許出願第９７９５０５号（ＩＢＭドケット番号ＡＭ９－９７－０５３）"SECURE CONFIGURATION OF A DIGITAL CERTIFICATE FOR APRINTER OR OTHER NETWORK DEVICE"（本願と同日出願）で開示される。このデジタル証明書は、文書ソースに対して、そのプリント・サーバがプリント・サーバが表すそれ自身であることを立証する。

【００３８】本発明の実施例が留置き証明書内に、プリンタのプリンタＩＤ及びネットワーク・アドレスのためのフィールドを含む場合（これらはユーザが留置き証明書に対する要求を発行することにより指定される）、文書ソースはまた、ファイルを要求しているプリンタが、ユーザにより文書ソースに対して指定されたのと同一のプリンタであることを確認できる。文書ソースはまた、印刷要求が、ユーザにより指定され、留置き証明書内に記録された同一のネットワーク・アドレスから発信されていることを確認できる。

【００３９】文書ソース１０が留置き証明書を受信するとき、文書ソース１０はこの証明書が実際に、自身により最初に発行されたものであるかを確認できる。文書ソースは、デジタル署名が自身だけがその私用キーを用いて生成できたものであることを認識している。留置き証明書の内容に対してハッシュ関数を用いることにより、デジタル署名が留置き証明書の内容にもとづくものであるという点で固有である場合、文書ソースはその私用キーをハッシュ値に対して使用することにより、デジタル署名を解読できる。文書ソースは次に、受信された留置き証明書の内容に同一のハッシュ関数を適用し、結果のハッシュを比較することにより、自身が留置き証明書に署名した後、留置き証明書内のデータ（例えばファイル名、プリンタＩＤなど）が変更されていないことを確認する。他の実施例、特に固有のデジタル署名を有さない実施例では、文書ソースは発行された各留置き証明書に対して、識別情報（検索されるファイル名及び要求ユーザにより最初に指定されたプリンタのＩＤなど）を、その留置き証明書の固有の通し番号に関連付けることにより、自身のログまたはデータベースを保持することができる。次に、留置き証明書が返信されるとき、文書ソースは留置き証明書内の通し番号を参照し、発行された留置き証明書内の情報が、受信された留置き証明書内の情報に合致するか否かを決定できる。

【００４０】プリンタがそれが主張する当該プリンタであることを確認し、留置き証明書が、文書ソースにより発行されたものから変更されていないことを確認した後、文書ソースは通信５を介して、文書を安全にプリンタに送信できる。

【００４１】ネットワーク環境：本発明の別の実施例が図３に示され、そこではプリント・サーバ３０が物理的に安全な環境Ａ内にあり、プリンタの出力への物理アクセスが、"ロック・アンド・キー"により、または他の類似の制御式アクセス手段、例えばパスワード・トリガ機構やバッジ・ロックなどを通じて制限される。ファイル・ソース・サーバ１０及びユーザ／クライアント２０は、同一の物理的に安全な環境内にあってもなくてもよく、或いは全く物理的に安全な環境内になくてもよい。同様に、プリンタ、クライアント及びサーバは、通信リンク５０が安全でないインターネットなどのネットワークに通信リンクされ得る。

【００４２】前述の本発明を使用すると、ユーザ２０は特定のファイルのために、サーバ１０から留置き証明書を要求する。要求と一緒に、ユーザ２０は信頼される当局からサーバ１０にユーザのデジタル証明書を送信する。サーバ１０が、要求ユーザが要求ファイルへのアクセスを有するか否かを判断するための、アクセス制御リストを有するデータベースを保持してもよいし、或いはアクセス権限がユーザのデジタル証明書の一部であってもよい。一旦サーバ１０が、ユーザ２０がファイルへのアクセスを許可されたと判断すると、サーバ１０は前述のように、自身がユーザのデジタル証明書内で受信したユーザの公開キーにより暗号化される留置き証明書を送信する。ユーザはユーザ自身の私用キーを用いて留置き証明書を解読し、それを後述のように、ユーザがプリンタのデジタル証明書から受信したプリンタの公開キーを用いて暗号化する。ユーザ２０は次に印刷要求を、暗号化された留置き証明書と一緒に、プリント・サーバ３０に送信する。この留置き証明書は、サーバの識別名、要求ファイルへのパス及びサーバの私用キーを用いて暗号化されたサーバのデジタル署名を含む。印刷システムが暗号化された留置き証明書を受信すると、プリンタがそれを印刷システムの私用キーを用いて解読する。

【００４３】図４は、印刷システム３０へのアクセスを制御するために、デジタル証明書が使用され得る様子を示す。プリンタ３０が特定種類のアクセス制御リストを有するか、アクセス権限が潜在ユーザ２０から受信されるデジタル証明書内で指定され得る。アクセスを要求するユーザが、そのユーザが主張する当人であることを認証することが必要であろう。プリンタを使用するためのセキュリティ取扱許可を有さないユーザから保護するこ

とに加え、他の無許可のユーザが単純な識別／パスワード機構を見破り、例えばフラッシュ・メモリ内の情報などの、プリンタの主要な構成情報を破壊し得る。

【００４４】アクセスを要求するユーザは、こうした要求をユーザの公開キーを含むユーザのデジタル証明書と一緒に、プリンタに送信する（４０１）。プリンタはユーザのデジタル証明書を認証するために、公開キー及びユーザ識別を証明書当局６０に送信する（４０２）。印刷システムは現在、ユーザの公開キーを有し、それが認証されていることを認識する。プリンタはユーザにランダム・メッセージを送信する（４０３）。ユーザはメッセージをその私用キーにより暗号化し、それをプリンタに返信する（４０４）。印刷システムが、メッセージをユーザの公開キーにより解読する。それがオリジナル・メッセージに合致する場合、印刷システムはユーザがそのユーザが主張する当人であることを認識する。

【００４５】アクセス特権は、管理上確立されたアクセス制御リスト（ＡＣＬ）に対してチェックされる。更に、ＡＣＬ内で許可された場合にだけ、オペレーションは許可される。例えば、許可された管理者だけが安全なメールボックスを準備し、プリンタを再構成し、新たなデジタル証明書をロードできる。オペレータはジョブを消去できるが、エンド・ユーザは印刷ジョブを依頼できるだけである。同様に、図３におけるユーザ２０のアクセス権限が確認される。

【００４６】図３を参照すると、プリンタはユーザ２０の認証及び権限を確認すると、プリンタはファイル要求を留置き証明書と一緒にサーバに送信する。その際、証明書はプリンタの私用キーにより暗号化される。プリンタはまたプリンタのデジタル証明書も送信する。プリンタのデジタル証明書は、前記米国特許出願第９７９５０５号（ＩＢＭドケット番号ＡＭ９－９７－０５３）"SECURE CONFIGURATION OFA DIGITAL CERTIFICATE FOR A PRINTER OR OTHER NETWORK DEVICE"で述べられるプロセスにより作成される。

【００４７】本質的にプリンタのデジタル証明書は、プリンタの製造者が製造の間に秘密キーをプリンタに組み込むプロセスにより作成される。プリンタの通し番号、プリンタのモデル番号及びキーは、プリンタの製造者などの証明書当局により保持される安全なデータベースに記録される。デジタル証明書が要求されるとき、プリント・サーバは２部分からなるメッセージを証明書当局に送信する。第１の部分は、プリンタの通し番号及びモデル番号を含み、第２の部分は、プリンタの組み込み秘密キーにより暗号化されたこれと同一の情報を含む。証明書当局は安全なデータベース内で、モデル番号及び通し番号を調査し秘密キーを見い出す。秘密キーは、メッセージの第２の部分を解読するために使用される。メッセージの第２の部分の解読部分が第１の部分に合致すると、プリンタは認証済みである。当局は次にデジタル証明書を秘密キーにより暗号化し、プリンタに送信する。当局は、プリンタに提供される証明書内に公開キーを含み、対応する私用キーをデータベースからの秘密キーにより暗号化する。暗号化された秘密キーは、デジタル証明書と一緒に、プリンタに送信される。１実施例では、プリンタに組み込まれ、当局のデータベースに記憶される秘密キーが、プリンタと当局との間でデジタル証明書を生成するために使用されるだけである。こうした実施例では、秘密キーが従来の対称暗号法を用いる他の通信には使用されない。しかしながら、他の実施例では実際、認証プロセスが幾分妥協され得ることを承知の上、他のこうした通信のために組み込み秘密キーを使用し得る。

【００４８】ファイル・サーバ１０が次に、プリンタからのデジタル証明書内で見い出される公開キーを用い、ファイル要求と一緒に留置き証明書を解読する。

【００４９】プリンタはまた第２の秘密キーを生成し、それを自身の私用キーを用いて暗号化し、サーバに送信できる。サーバは次に秘密キーを、プリンタのデジタル証明書からの公開キーを用いて解読する。別の実施例では、サーバが秘密キーを生成し、それをプリンタの公開キーを用いて暗号化してプリンタに送信する。サーバは秘密キーまたはプリンタの公開キーのいずれかを用い、ファイルを暗号化する。ファイル・サーバは暗号化されたファイルをプリンタに送信する。プリンタはファイルを適切なキーを用いて解読する。ある実施例は、このアプローチを使用する。なぜなら、公開キー暗号化は秘密キー暗号化よりも遅いからである。従って、秘密キー暗号化がサーバにより大量の文書に対して使用され、解読がプリンタにより実行され得る。この時、プリンタは同一の秘密キーを用いてファイルを解読できる。

【００５０】暗号文実施例：以下では、電子商取引環境において、文書の安全な印刷を提供するための、暗号文及び留置き証明書の１つの可能な使用について述べる。電子商取引が台頭する社会において、出版業者はしばしば、丁度印刷本または雑誌の１コピーを販売するように、単一の印刷コピーだけに対する権利を販売したいと思う。文書の印刷可能なバージョンが、システム内のどこにでも明文で存在することを可能にすると、出版業者を危険に晒すことになる。なぜなら、不正なコピーが生成され、何度も印刷され得るからである。たとえ暗号化された文書がスプールされ、プリンタに到達する途中で解読されても、システムは実のプリンタをソフトウェアにより置換することにより、だまされ得る。従って、この環境のプリンタは、プリンタがそれら自身を認証し、固有の公開暗号キーを提供し、標準の解読アルゴリズムを用いて、文書をオン・ザ・フライ式に解読及び印刷することが可能なように、安全であるべきである。

【００５１】図５を参照すると、エンド・ユーザ２０は、ユーザが文書の印刷可能なコピーを購入したいこと

を判断する（５０１）。このバージョンは、フォーマットや高品質イメージ及びフォントの使用などの点で、印刷不能なバージョンとは異なる。多分、著作権の保護がすき込まれるであろう。購入取引の一部として、エンド・ユーザはこの文書を購入するために、ユーザ自身が認証済みの安全なプリンタへのアクセスを有さねばならず、またプリンタの公開キー証明書を提供しなければならないことを告げられる（５０２）。ユーザは次にＳＮＭＰ獲得を用い、プリンタから証明書を獲得する（５０３）。ここでプリンタの公開キー証明書は、プリンタ内のＳＮＭＰ　ＭＩＢに記憶されるものと仮定する（５０４）。前述のように、プリンタの公開キー証明書は、プリンタを認証するのに必要な情報と一緒に、プリンタの公開暗号キーを含む。これは重要なステップである。なぜなら、出版業者は、プリンタがユーザが主張する当該プリンタであることを保証されなければならないからである。証明書が出版業者に送信される（５０５乃至５０７）。

【００５２】出版業者は、留置き証明書をユーザに送信する（５０８）。ユーザは留置き証明書及び出版業者のＵＲＬをプリント・サーバに送信する（５０９）。プリンタは、印刷ファイルを獲得するために、留置き証明書及びプリンタ証明書を含むメッセージを、出版業者／サーバに送信する（５１５）。

【００５３】出版業者は文書のための暗号文を作成し、それをユーザに送信する。文書自体は対称キーにより暗号化され、そのキーがプリンタの公開キーを用いて暗号化される（５２０）。

【００５４】暗号文化された文書がプリント・サーバに送信され、そこで印刷される。プリント・サーバは暗号化文書をスプール上に配置し（５２５）、プリンタがそれを要求するまで暗号キーを保持する。

【００５５】プリンタは新たな印刷ジョブを要求し、暗号化文書がプリンタ５３０に送信される（５３０）。プリンタはこれが暗号化文書であることを理解し、プリント・サーバからキーを要求する（５３５）。サーバはキーを送信し（５４０）、キー自身がプリンタの公開キーを用いて暗号化される。プリンタはキーを解読し、そのキーを用いて文書を解読し、印刷する。

【００５６】前述の仕様に従い、本発明はプログラミング・ソフトウェア、ファームウェア、ハードウェアまたはそれらの任意の組み合わせを生成するための、標準のプログラミング技術及びエンジニアリング技術を用いることにより、マシン、プロセスまたは装置として実現される。

【００５７】コンピュータ読出し可能プログラム・コードを有する任意の結果のプログラムが、メモリ装置または伝送装置などの、１つ以上のコンピュータ使用可能媒体内で実現され、それにより本発明に従うコンピュータ・プログラム製品または装置を形成する。ここで、本明細書で使用される用語"装置（article of manufacture）"及び"コンピュータ・プログラム製品"は、メモリ装置上または伝送装置内などの任意のコンピュータ使用可能媒体上に、（永久的にまたは一時的に）存在するコンピュータ・プログラムを包含するように意図される。

【００５８】ある媒体からのプログラム・コードの直接実行、媒体上へのプログラム・コードの記憶、ある媒体から別の媒体へのコードのコピー、伝送装置によるコードの伝送または他の等価な操作は、メモリまたは伝送装置を使用する。そして、これらのメモリまたは伝送装置は、本発明を形成もしくは使用する、または販売する際の予備ステップまたは最終ステップとして、プログラム・コードを一時的に具体化するだけである。

【００５９】メモリ装置は、固定（ハード）ディスク・ドライブ、ディスケット、光ディスク、磁気テープ及びＲＡＭ、ＲＯＭ、ＰＲＯＭなどの半導体メモリを含む。伝送装置は、インターネット、イントラネット、電子掲示板及びメッセージ／短信交換、電話／モデム・ベースのネットワーク通信、配線式／ケーブル式通信ネットワーク、セルラ通信、無線通信、衛星通信及び他の静止または移動ネットワーク・システム／通信リンクを含む。

【００６０】本発明を実現するマシンは１つ以上の処理システムを含み、それらにはＣＰＵ、メモリ／記憶装置、通信リンク、通信／伝送装置、サーバ、Ｉ／Ｏ装置、プリンタまたは本発明を実現する１つ以上の処理システムの任意のサブコンポーネントまたは個々のパーツ、例えばソフトウェア、ファームウェア、ハードウェアまたはそれらの任意の組み合わせが含まれる。

【００６１】コンピュータ・サイエンスに関わる当業者であれば、前述のように作成されるソフトウェアを、適切な汎用のまたは特殊目的のコンピュータ・ハードウェアと組み合わせることにより、本発明を実現するコンピュータ・システムもしくは印刷システムまたはサブコンポーネント、並びに本発明の方法を実現するコンピュータ・システムもしくは印刷システム、またはサブコンポーネントを容易に形成することができよう。

【００６２】本明細書では、用語"ファイル"及び"文書"は交換可能に使用され、このことは任意の文書はファイルでもあるが、ファイルは必ずしも文書に限らないことを意味する。たとえ用語"文書"が使用される場合にも、そのより広い"ファイル"の意味が意図される。なぜなら、用語"文書"は、本明細書では単にファイルの１例として使用されるからである。

【００６３】また、本明細書では、用語"プリンタ"、"プリント・サーバ"及び"印刷システム"は交換可能に使用される。プリンタの機能について述べられるとき、プリンタは、コンピュータに接続されるスタンドアロン・プリンタ、すなわち印刷システムや、プリント・サーバまたはプリンタ制御装置などの機能を実行するために必要な能力に接続されているものと仮定する。更に、ファ

ックス・マシンも本発明の状況においては、プリンタであると理解され得る。

【００６４】また、用語"ファイル・サーバ"、"ファイル・ソース"などは、本明細書では漠然と使用される。任意のこうした参照は、ファイルが存在する記憶装置を制御する任意のコンピュータ・システムを意味する。サーバは、クライアント／サーバ技術の意味で、専用の"サーバ"である必要はないが、勿論そうであってもよい。同様に、用語"クライアント"は、本明細書ではリクエスタを意味するために漠然と使用されるが、必ずしもクライアント／サーバ環境におけるクライアントに典型的な、特定のハードウェアまたはソフトウェア構成を意味しない。しかしながら、こうした意味合いが除外されるわけではない。

【００６５】まとめとして、本発明の構成に関して以下の事項を開示する。

【００６６】（１）インターネットを介して、ファイル・サーバに存在するファイルを印刷する方法であって、第１のコンピュータ・システムにより前記ファイル・サーバに、前記ファイルを印刷する権限を要求するステップと、前記要求に応答して、前記ファイル・サーバから前記第１のコンピュータ・システムに、前記第１のコンピュータ・システムのインターネット・アドレスを含む、前記ファイルを要求するためにプリント・サーバにより必要とされ、該プリント・サーバに転送される情報を含む証明書を発行するステップと、前記証明書を前記第１のコンピュータ・システムから前記プリント・サーバに送信するステップと、前記プリント・サーバから前記ファイル・サーバに、前記ファイルを要求し、前記ファイルを受信する権限として前記証明書を含むメッセージを送信するステップと、前記証明書の内容から、含まれる前記証明書が、前記第１のコンピュータ・システムに発行されたのと同一の証明書であることを確認後、前記ファイル・サーバから前記プリント・サーバに前記ファイルを送信するステップとを含む、方法。

（２）インターネットを介して通信接続される第１のコンピュータ・システム、プリント・サーバ及びファイル・サーバを含むネットワーク・システムであって、第１のコンピュータ・システムにより前記ファイル・サーバに、ファイルを印刷する権限を要求する手段と、前記要求に応答して、前記ファイル・サーバにより前記第１のコンピュータ・システムに発行され、前記ファイル・サーバのデジタル署名及び前記ファイル・サーバのインターネット・アドレスを含む、前記ファイルを要求するために前記プリント・サーバにより必要とされる情報を含む証明書と、前記第１のコンピュータ・システムから前記プリント・サーバに前記証明書を送信する手段と、前記プリント・サーバから前記ファイル・サーバに、前記ファイルを要求し、前記ファイルを受信する権限として前記証明書を含むメッセージを送信する手段と、前記ファイル・サーバにより前記証明書の内容から、含まれる前記証明書が、前記第１のコンピュータ・システムに発行されたのと同一の証明書であることを確認する手段と、前記ファイル・サーバから前記プリント・サーバに前記ファイルを送信する手段とを含む、ネットワーク・システム。

（３）第１のコンピュータ・システム内で実行される方法であって、ファイル・サーバに存在するファイルをネットワークを介してリモート・プリンタにより印刷する要求を、前記ネットワークを通じて、前記ファイル・サーバに送信するステップと、前記ファイル・サーバから前記ネットワークを通じて、前記ファイル・サーバのデジタル署名を含む、前記ファイルを印刷するための権限を受信するステップと、前記権限を前記ネットワークを通じて前記プリンタに渡し、該プリンタが続いて前記ファイルを前記ファイル・サーバから直接フェッチし、印刷することを可能にするステップとを含む、方法。

（４）ファイル・サーバに存在するファイルをリモート・プリンタにより印刷する要求を、ネットワークを通じて前記ファイル・サーバに送信する手段と、前記ファイル・サーバから前記ネットワークを通じて受信され、前記ファイル・サーバのデジタル署名を含む、前記ファイルを前記ネットワークを通じて前記リモート・プリンタにより印刷するための権限と、前記権限を前記ネットワークを通じて前記プリンタに渡し、該プリンタが続いて前記ファイルを前記ファイル・サーバから直接フェッチし、印刷することを可能にする手段とを含む、第１のコンピュータ・システム。

（５）前記権限が前記ファイルの位置に関する情報を含む、前記（４）記載のシステム。

（６）前記権限が前記ファイル・サーバの識別名及び前記ファイルのパスを含む、前記（４）記載のシステム。

（７）ファイル・サーバ内で実行される方法であって、第１のコンピュータ・システムからの、前記ファイル・サーバに存在するファイルへのアクセス権限に対する要求に応答して、第１のコンピュータ・システムからネットワークを通じてプリント・サーバに渡される、前記ファイル・サーバのデジタル署名を内容に含む権限の証明書を与えるステップと、印刷のために前記ファイルへの直接アクセスを要求する前記プリント・サーバから、前記ネットワークを通じて、前記権限の証明書を受信するステップと、前記証明書の内容を通じて、前記証明書が前記第１のコンピュータ・システムに与えられたのと同一の無変更の証明書であることを確認するステップと、前記ファイルを前記プリント・サーバに送信するステップとを含む、方法。

（８）リモート・プリント・サーバによるファイル・サーバに存在するファイルへの、ネットワークを介するアクセス権限のための要求を、第１のコンピュータ・システムから受信する手段と、前記要求に応答して作成さ

れ、前記ファイルをアクセスするために前記プリント・サーバにより必要とされる情報及びデータ構造の妥当性を保証するために前記ファイル・サーバにより必要とされる情報を含む、コンピュータ読出し可能媒体上のデータ構造と、前記データ構造を前記第１のコンピュータ・システムに送信する手段と、印刷のために前記ファイルへの直接アクセスを要求する前記プリント・サーバから、前記ネットワークを通じて、前記データ構造を受信する手段と、前記データ構造の内容を通じて、証明書が前記第１のコンピュータ・システムに送信されたのと同一の無変更のデータ構造であることを確認する手段と、前記ファイルを前記プリント・サーバに送信する手段とを含む、ファイル・サーバ。

（９）前記データ構造が前記ファイル・サーバのデジタル署名を含む、前記（８）記載のファイル・サーバ。

（１０）前記データ構造が前記ファイル・サーバの識別名、前記ファイルのパス、前記ファイル・サーバのデジタル署名、有効日及び前記ファイル・サーバにより作成された前記データ構造の固有番号を含む、前記（８）記載のファイル・サーバ。

（１１）前記データ構造が、前記要求内で指定されるプリント・サーバのプリンタＩＤ及びネットワーク・アドレスを含む、前記（８）記載のファイル・サーバ。

（１２）プリント・サーバ内で実行される方法であって、第１のコンピュータ・システムのために、前記第１のコンピュータ・システムからネットワークを介して、ファイル・サーバからネットワークを介してファイルを検索し、前記プリント・サーバにより印刷するための要求を受信するステップと、前記要求と共に、前記ファイルを突き止め、前記ファイルを検索して印刷する前記ファイル・サーバからの権限を保証するために、前記プリント・サーバにより必要とされる情報を含む証明書を受信するステップと、前記証明書を前記ネットワークを介して前記ファイル・サーバに送信するステップと、前記ファイルを前記ファイル・サーバから受信するステップとを含む、方法。

（１３）第１のコンピュータ・システムのために、前記第１のコンピュータ・システムからネットワークを介して、ファイル・サーバからネットワークを介してファイルを検索し、プリント・サーバにより印刷するための要求を受信する手段と、前記要求と共に受信され、前記ファイルを突き止め、前記ファイルを検索して印刷する前記ファイル・サーバからの権限を保証するために、前記プリント・サーバにより必要とされる情報を含む、コンピュータ使用可能媒体上に存在するデータ構造と、前記データ構造を前記ネットワークを介して前記ファイル・サーバに送信する手段と、前記ファイルを前記ファイル・サーバから受信して印刷する手段とを含む、プリント・サーバ。

（１４）前記権限を保証するために必要とされる情報が、前記ファイル・サーバのデジタル署名である、前記（１３）記載のプリント・サーバ。

（１５）第１のコンピュータ・システム、第２のコンピュータ・システム及び第３のコンピュータ・システムのネットワークを介して実行される方法であって、前記第２のコンピュータ・システムから前記第１のコンピュータ・システムに、ファイル検索のための権限を要求するステップと、前記要求に応答して、前記第１のコンピュータ・システムから前記第２のコンピュータ・システムに、前記ファイルを要求するために前記第３のコンピュータ・システムにより必要とされる情報を含み、前記第３のコンピュータ・システムに渡され、前記第１のコンピュータ・システムにより認証される証明書を発行するステップと、前記第２のコンピュータ・システムから前記第３のコンピュータ・システムに、前記証明書及び前記ファイルの検索要求を送信するステップと、前記第３のコンピュータ・システムから前記第１のコンピュータ・システムに、前記ファイルを要求し、該ファイルを受信する権限として前記証明書を含むメッセージを送信するステップと、前記第１のコンピュータ・システムにより、含まれる前記証明書が、前記第２のコンピュータ・システムに発行されたのと同一で無変更の証明書であることを確認するステップと、前記証明書が確認された場合、前記ファイルを前記第３のコンピュータ・システムに送信するステップとを含む、方法。

（１６）印刷のために互いに通信リンクされる第１、第２及び第３のコンピュータ・システムを有するネットワーク・システムであって、前記第３のコンピュータ・システムがプリンタを有し、ファイル・ソースを有するサーバとして機能する前記第１のコンピュータ・システムにファイルが存在するものにおいて、前記第２のコンピュータ・システムから前記第１のコンピュータ・システムに、ファイルを印刷するための権限を要求する手段と、前記要求に応答して、前記第１のコンピュータ・システムから前記第２のコンピュータ・システムに、前記ファイルを要求するために前記第３のコンピュータ・システムにより必要とされる情報を含み、前記第３のコンピュータ・システムに渡され、前記第１のコンピュータ・システムにより認証される証明書を発行する手段と、前記第２のコンピュータ・システムから前記第３のコンピュータ・システムに、前記証明書及び前記ファイルの印刷要求を送信する手段と、前記第３のコンピュータ・システムから前記第１のコンピュータ・システムに、前記ファイルを要求し、該ファイルを受信する権限として前記証明書を含むメッセージを送信する手段と、前記第１のコンピュータ・システムにより、含まれる前記証明書が、前記第２のコンピュータ・システムに発行されたのと同一で無変更の証明書であることを確認する手段と、前記証明書が確認された場合、前記ファイルを前記第３のコンピュータ・システムに送信する手段とを含

む、システム。

（１７）前記証明書が前記ファイルが記憶される位置の識別名を含む、前記（１６）記載のシステム。

（１８）前記識別名が前記ファイルが記憶される位置のインターネット・アドレスを含む、前記（１７）記載のシステム。

（１９）前記証明書が前記ファイルへのパスを含む、前記（１６）記載のシステム。

（２０）前記証明書が前記第１のコンピュータ・システムのデジタル署名を含む、前記（１６）記載のシステム。

（２１）前記第３のコンピュータ・システムがプリント・サーバである、前記（１６）記載のシステム。

（２２）前記第３のコンピュータ・システムが印刷システムである、前記（１６）記載のシステム。

（２３）前記第３のコンピュータ・システムがファックス・マシンである、前記（１６）記載のシステム。

（２４）前記第１のコンピュータ・システムが、前記ファイルが存在するファイル・データベースを含む、前記（１６）記載のシステム。

【図面の簡単な説明】

【図１】”留置き”証明書が通信の一部内に含まれる、ユーザ、文書ソース及びプリント・サーバの間の情報の流れを示す図である。

【図２】留置き証明書の構造を示すブロック図である。

【図３】ネットワーク構成を示す図である。

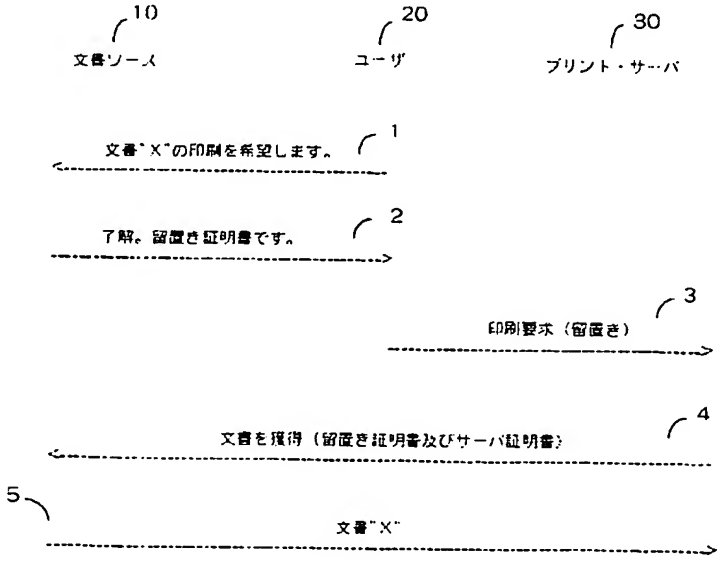
【図４】デジタル証明書を用い印刷システムへのアクセスを制御する、ユーザ、印刷システム及び証明書当局の間の情報の流れを示す図である。

【図５】暗号文及び留置き証明書を用い、ユーザ、デジタル・ライブラリ・ファイル・ソース、プリント・サーバ及びプリンタ間の情報の流れを示す図である。

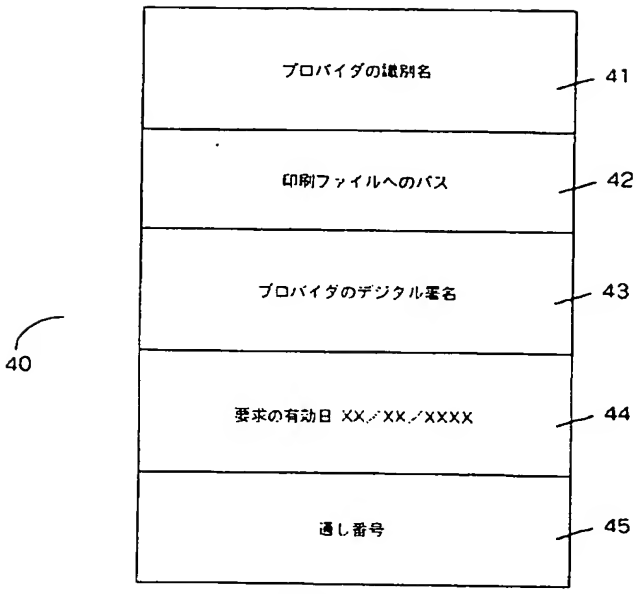
【符号の説明】

１、２、３、４、５　通信
１０　文書ソース
２０　ユーザ（クライアント）
３０　プリント・サーバ
４０　留置き証明書
４１　識別名
４２　パス
４３　デジタル署名
４４　日付
４５　通し番号
５０　通信リンク
６０　証明書当局

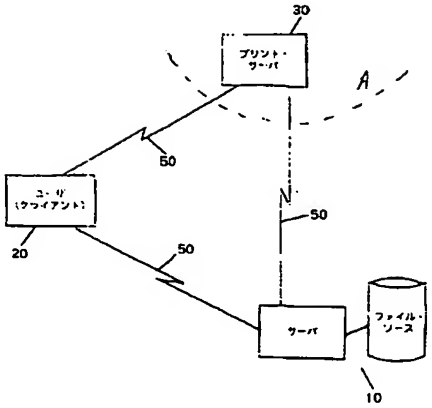
【図１】



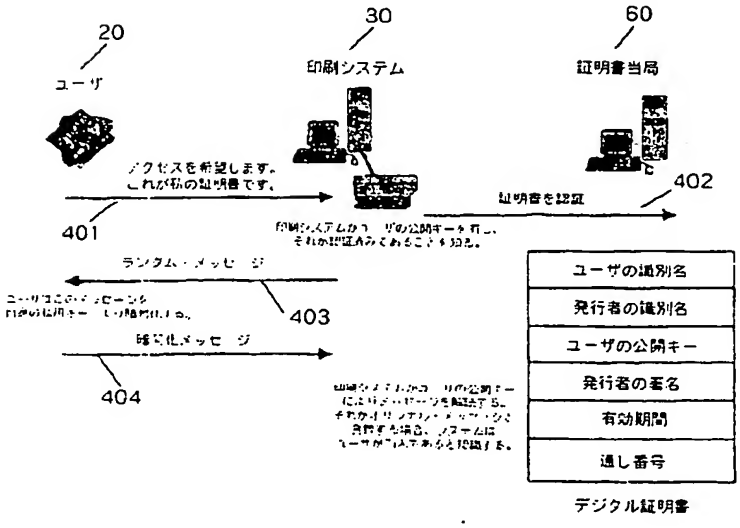
【図２】



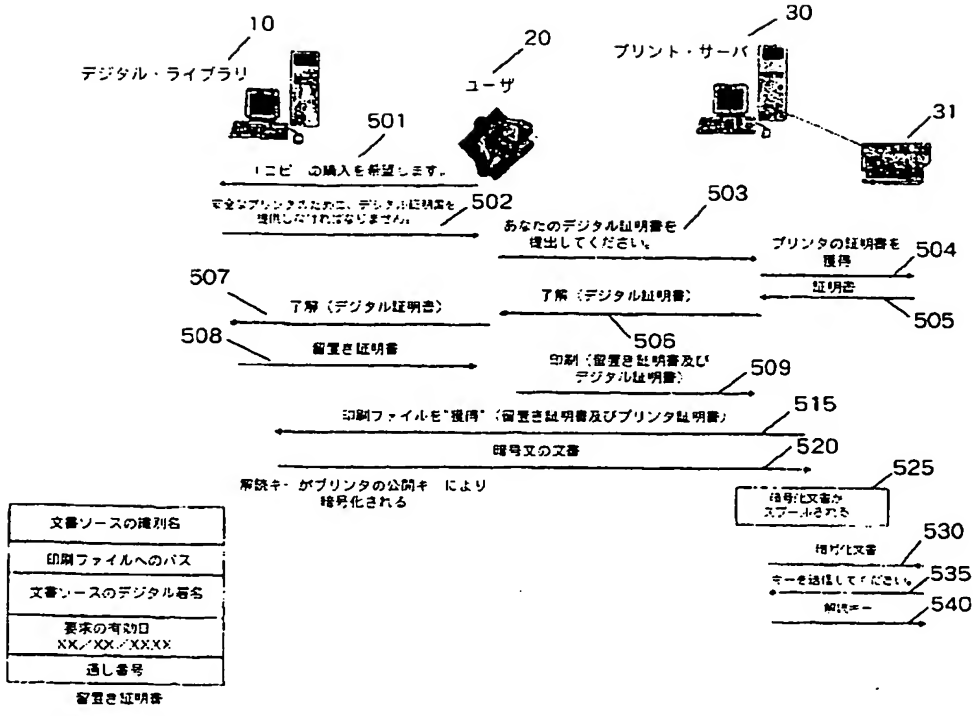
【図３】



【図４】



【図５】



フロントページの続き

(56)参考文献　特開　平８－335208（ＪＰ，Ａ）
特開　平９－44429（ＪＰ，Ａ）
特開　平11－25048（ＪＰ，Ａ）
電子情報通信学会論文誌　Ｖｏｌ．Ｊ79－Ｄ－２　Ｎｏ．10　ｐ．656－ｐ．668「組織構造に基づく権限の委譲を伴った分散オブジェクトモデル」飯島正

(58)調査した分野(Int.Cl.7，ＤＢ名)
G06F　3/12
G06F　13/00　357
G06F　15/00　330
H04L　9/32